

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2012

Date filed: February 26, 2013

Name of company covered by this certification: HyperCube Telecom, LLC

Form 499 Filer ID: 824874

Name of signatory: Ronald R. Beaumont

Title of signatory: President

I, Ronald Beaumont, certify that I am an officer of HyperCube Telecom, LLC ("HyperCube" or the "Company"), and acting as an agent of HyperCube, that I have personal knowledge that HyperCube has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how HyperCube's procedures ensure that the Company is in compliance with the requirements (including, where applicable, those mandating the adoption of CPNI procedures, record keeping and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

HyperCube has not taken any actions (i.e., proceedings instituted or petitions filed by HyperCube at either state commissions, the court system, or at the Commission) against data brokers in the past year, nor is there any evidence that pretexters attempted to access CPNI maintained by HyperCube.

The Company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

A handwritten signature in black ink that reads "Ronald Beaumont". The signature is stylized with a large, sweeping horizontal stroke at the end.

Signed

Ronald R. Beaumont

President

HyperCube Telecom, LLC

HYPERCUBE TELECOM, LLC STATEMENT OF COMPLIANCE WITH CPNI RULES

HyperCube Telecom, LLC ("HyperCube" or the "Company") is a competitive telecommunications carrier providing wholesale services to other telecommunications carriers and application service providers that are designed to broaden and enhance their ability to interconnect their respective networks and allow them to exchange traffic with one another more effectively and efficiently. The Company's operations are focused on the provision of tandem switching and transport services to wireless carriers, interexchange carriers, competitive local exchange carriers and incumbent local exchange carriers.

The Company only has access to limited forms of CPNI from its wholesale carrier customers and has adopted various operational procedures to assure that, consistent with the Commission's rules, all of the CPNI that it holds is protected from unauthorized and unlawful use, access and disclosure.

Consistent with the CPNI rules, the Company may use, disclose and permit access to CPNI without customer approval (1) to render, bill and collect for services provided; (2) to protect rights or property of the Company, other users or other carriers from unlawful use; (3) for the purpose of network maintenance, repair and troubleshooting; and (4) to comply with a valid legal process such as a subpoena, court order, or search warrant.

The Company does not use, disclose or permit access to CPNI for marketing purposes other than for the purpose of providing service offerings for the type of services to which the Company's customer already subscribes. It is therefore not required to seek approval from existing customers to use their CPNI and does not maintain a record of a customer's approval to use CPNI. In the event the Company changes its marketing practices or expands its service offerings so that customer approval is required, it will implement a system by which customers will be notified of such use and the status of a customer's CPNI approval can be clearly established prior to the use of CPNI. Furthermore, the Company does not share, sell, lease and otherwise provide CPNI to any of its affiliates, suppliers, vendors and any other third parties for the purposes of marketing any services.

The Company has effectuated processes and procedures to train its personnel as to when they are and are not permitted to use CPNI and has completed such training and will periodically refresh such training (at minimum, annually). For instance, all Company employees receive CPNI training and are required to abide by the Company's CPNI Protection Policy, which, *inter alia*, requires employees to maintain the confidentiality of all information, including CPNI, which may be obtained as a result of their employment by the Company. The Company's CPNI Protection Policy also provides a comprehensive roadmap of how Company employees are required to use, maintain and disclose CPNI. Employees who violate the Company's CPNI Protection

Policy are subject to disciplinary action, ranging from written warnings to discharge, depending on the nature, frequency, and severity of the violation(s) including possible termination.

To the extent the Company engages in any marketing campaigns, it has established a supervisory review and approval process to ensure that such campaigns are consistent with FCC's CPNI rules. The Company maintains a record for at least one year of its own and, if applicable, affiliates' sales and marketing campaigns, if any, that use customers' CPNI.

The Company does not provide its wholesale customers or their customers CPNI without proper customer authentication on inbound telephone calls, in accordance with contractual arrangements. The Company only discusses over the phone call, information of its wholesale customers' end user customers that is provided by the wholesale customer. With respect to call detail information pertaining to end users of the Company's wholesale customers' services, the Company uses the information in switch records that are generated when the Company provides its tandem and transport services to bill for such services. The information in these switch records is not organized in a manner that would allow the Company to identify any individual end user customers and the Company only shares that information with its wholesale customers who are properly authenticated and then only by sending those records to the applicable customer's address of record. All Company customers have dedicated account representatives who serve as the primary customer contact. The account representatives personally know each customer. Currently the Company does not provide in-store account access for its customers.

If a customer's address changes, the Company will notify the customer of that change by mailing such notice to the customer's address of record consistent with the FCC's CPNI rules. In the event of a breach of CPNI that is maintained by the Company, it will provide law enforcement with electronic notice of such CPNI breach as soon as practicable and not later than 7 business days after reasonable determination of the breach. After notifying law enforcement and unless directed otherwise, the Company will notify affected customers not earlier than 7 full business days later and will maintain a record of any CPNI-related breaches and the related notifications for a period of at least 2 years as required by the applicable FCC CPNI rules.

In the event that the Company changes its marketing practices such that opt-out notices are required, the Company will implement procedures whereby it will provide the FCC written notice within 5 business days of any instance where the opt-out mechanisms do not work properly, to such a degree that customers' inability to opt-out is more than an anomaly.

HYPERCUBE TELECOM, LLC
CUSTOMER PROPRIETARY NETWORK INFORMATION (“CPNI”)
PROTECTION POLICY

Table of Contents	1
I. Overview	2
II. What is CPNI?	4
III. Use of CPNI Without Customer Consent	5
IV. When Must a Customer be Authenticated?	5
V. When is Hypercube Required to Disclose CPNI?	6
VI. Confidentiality Agreements with Contractors and Joint Venture Partners	6
VII. Retention and Win-Back	7
A. Restrictions on use of Carrier Proprietary Information to retain customers	7
B. Win-back	7
VIII. Training and Reporting	8
A. Training Requirements	8
B. Reporting Requirements	8
C. Notification of Account Changes	8
IX. Record-Keeping Requirements	9
X. Breach Notification	9
XI. How May CPNI be Used with the Customer’s Approval and How That Approval Must be Obtained	9
A. Opt-Out Approval	10
B. Opt-In Approval	10
XII. Notice Requirements Applicable to Both Opt-In and Opt-Out Methods of Approval	11
XIII. Special Requirements Applicable to One-Time Oral Notices to Customers	11
XIV. How to Verify a Customer’s Approval and Obtain Supervisory Approval for Proposed Outbound Marketing Efforts	11
A. Customer Approval Database	11
B. Supervisory Review Required Before Making a Request to a Customer	12
XV. Glossary	13

HYPERCUBE TELECOM, LLC
CUSTOMER PROPRIETARY NETWORK INFORMATION ("CPNI")
PROTECTION POLICY

I. Overview

All HyperCube Telecom, LLC ("HyperCube" or "Company") employees, as well as all HyperCube agents and representatives, are required to comply with HyperCube's Customer Proprietary Network Information ("CPNI") Protection Policy ("CPNI Policy") which includes an obligation to maintain the confidentiality and security of all CPNI.

Both Congress and the Federal Communications Commission (FCC) impose requirements on telephone companies and VoIP providers about how they may use CPNI information and what they must do to protect it from disclosure. As CPNI is subject to detailed regulation, HyperCube's compliance with the regulatory requirements is mandatory.

The objectives of this document are to establish and/or reinforce HyperCube's policies and practices in connection with its treatment of CPNI and to provide information to HyperCube's employees, agents and representatives about their responsibilities relating to CPNI.

CPNI includes information about the types of telecommunications service a customer purchases, the amount and usage of a customer's telecommunications service, and information on a customer's bill. All of this information is considered confidential. All HyperCube employees are obligated to protect the confidentiality of CPNI and HyperCube employees are expressly forbidden from sharing or otherwise disclosing CPNI to anyone outside the Company unless required to do so to provide telecommunications services to the Company's customers or otherwise required by law. HyperCube supports all Federal and state laws and regulations that require the protection of CPNI, and all HyperCube employees must abide by these laws.

Generally, CPNI may be used without a customer's express approval to provide telecommunications services and to bill and collect for services rendered. CPNI also may be used to assist with any inbound telemarketing or administrative service for the duration of the customer's call, if the customer orally approves use of CPNI in this manner. The Human Resources Department will provide a means for all employees to receive training in the proper uses of CPNI. Anyone who has not received the required training should contact HyperCube's CPNI Contacts identified in the box below. New employees entering job positions that allow them access to CPNI will receive training with regard to CPNI requirements as part of their new hire orientation.

HYPERCUBE TELECOM, LLC
CUSTOMER PROPRIETARY NETWORK INFORMATION ("CPNI")
PROTECTION POLICY

All employees may access the HyperCube CPNI Protection Policy at Z:\Departments\Regulatory\Hypercube's Policies and Procedures and will be notified, as necessary, when a change occurs in Federal or state regulations that subsequently changes HyperCube's obligations.

The complete details of the Company's CPNI Protection Policy follow. All employees must read this policy and acknowledge that they have read it, understand it and agree to abide by it by signing the CPNI Protection Policy Acknowledgement Form attached to this policy. Please keep this document *for future reference and use*. Employees may at any time direct questions to the CPNI Policy Administrator or to HyperCube's Human Resources Manager, as follows.

HyperCube's CPNI Contacts:

CPNI Policy Administrator: Karen Turner (469) 727-1631

Mgr. Administration & H.R.: Carol Chauncey (469) 727-1516

HYPERCUBE TELECOM, LLC
CUSTOMER PROPRIETARY NETWORK INFORMATION ("CPNI")
PROTECTION POLICY

II. WHAT IS CPNI?

CPNI is defined by Federal statute [47 United States Code § 222(h)(1)]:

The term "customer proprietary network information" means—

(A) information that relates to the quantity, technical configuration, type, destination, location and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and

(B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; except that such term does not include Subscriber List Information.

CPNI includes most information that HyperCube collects about a customer because of their purchase of telecommunications services from us; this includes:

- Information about the **types** of service a customer buys, such as the technical configuration, destination and location of services a customer purchases from HyperCube. This may include design layout reports, service addresses, originating and terminating locations, circuit speed and capacity, etc.
- Information about the **amount** of service a customer purchases from HyperCube. For example, this may include the number of lines, circuits, calls, minutes, or the amount of equipment, subscribed to by the customer.
- Information about a customer's **usage** of telecommunications services, including numbers called, calls received, and optional features utilized.
- Information contained in a bill sent to the customer by HyperCube.
- Information contained in switch records generated when HyperCube provides its tandem and transport services to customers.

CPNI does *not* include:

- (i) subscriber list information, (ii) customer name, address and telephone number, or (iii) aggregate customer information.
- Subscriber List Information. This is a defined term under Federal law, and it means any information of a HyperCube subscriber (such as name, address, telephone number or classification) that the Company or an affiliate has published, caused to be published, or accepted for publication in a directory. While Subscriber List Information is not CPNI, HyperCube does require that third party vendors, partners and sales and marketing agents maintain the confidentiality of this information.

HYPERCUBE TELECOM, LLC
CUSTOMER PROPRIETARY NETWORK INFORMATION (“CPNI”)
PROTECTION POLICY

III. USE OF CPNI WITHOUT CUSTOMER CONSENT

- It is the Company’s policy to use CPNI only (i) to render, bill, and collect for services provided by the Company, (ii) to protect the Company’s rights and property, (iii) to protect the public and other carriers from the unlawful or fraudulent use of the Company’s services and (iv) for purposes of network maintenance, repair, and troubleshooting. Customer consent is not necessary to use CPNI in this manner.
- The Company also is permitted to provide access to CPNI to provide call location information in connection with 911 calls.
- The Company is restricted in how it may use CPNI to market services within service categories and among different service categories; the FCC recognizes three categories of telecom services: 1) local, 2) inter-exchange, and 3) CMRS, i.e., mobile wireless:
 - Marketing Within a Service Category: CPNI may be used, without notice or approval, for marketing HyperCube’s services within a single category of services to which the customer already subscribes. For example, if a customer already subscribes only to HyperCube’s local service, the Company may, without notice or approval, use that customer’s CPNI for the purpose of marketing additional local services, but not inter-exchange services or CMRS services.
 - Marketing Among Different Service Categories (“Total Services Approach”): When the customer buys services from more than one category in a bundle (see the three categories above), CPNI can be used without notice or approval only within the service categories already represented in the bundle. For example, if a customer subscribes to HyperCube’s local *and* interexchange services in a bundle, then HyperCube may, without notice or approval, use that customer’s CPNI for the purpose of marketing additional bundled local/interexchange services (HyperCube’s toll-free termination service is a bundled local/interexchange service). HyperCube is not permitted to use CPNI to cross-market into a service category from which the customer makes no purchase.
- It is against Company policy to use CPNI except (i) in accordance with the preceding paragraphs and (ii) upon written customer request.

IV. WHEN MUST A CUSTOMER BE AUTHENTICATED?

A customer must be authenticated *when the customer initiates a call to HyperCube and asks for CPNI* in the context of that telephone call.

- HyperCube will not share CPNI with customers on customer-initiated calls without authenticating the customer first. In the case of CPNI ***other than Call***

HYPERCUBE TELECOM, LLC
CUSTOMER PROPRIETARY NETWORK INFORMATION ("CPNI")
PROTECTION POLICY

Detail Information, this authentication should involve confirming that either (i) the customer already has substantial knowledge about the account (e.g., account numbers, passwords (if applicable), the type of existing services provided by HyperCube to the customer, the fact that an outage or service trouble may exist with respect to a particular service and is being reported by the customer) or (ii) is otherwise already known to HyperCube as a representative of the customer.

- With respect to Call Detail Information, if **any** customer requests to obtain such usage information on an inbound call – such as numbers called, calls received, time, location, or duration of any calls, and optional features utilized – no such information may be given to the calling customer over the phone. Instead, **all** HyperCube representatives only will send Call Detail Information to the customer at the customer's physical or electronic address of record or telephone number of record so long as those records have been associated with the customer's account for at least thirty (30) days.
- Nothing prevents a HyperCube employee from discussing Call Detail Information with a customer *where the customer provides that information and the conversation is limited to such customer-provided call detail information*.
- Customer Service Representatives or Account Representatives who receive inbound calls from customers shall be allowed to access CPNI after receiving oral permission from the customer if the customer can provide specific detail about the reason for their call (e.g. when disputing a phone charge, if the customer provides date/time of the charge in question, the HyperCube representative may discuss that charge), and such permission shall be limited to the duration of the call. The HyperCube representative shall note on the account that the customer gave one-time oral permission to access CPNI, and that the permission ended when the call ended.

V. WHEN IS HYPERCUBE REQUIRED TO DISCLOSE CPNI?

- HyperCube must provide CPNI to any person designated by the customer, upon receipt of an affirmative written request from the customer. In general, the Company cannot encourage a customer to freeze third-party access to CPNI.
- When required by law. If you believe HyperCube is required by law, such as through a subpoena or other request from law enforcement, to disclose CPNI, you must notify HyperCube's CPNI Policy Administrator as identified in the box on Page 3.

VI. CONFIDENTIALITY AGREEMENTS WITH CONTRACTORS AND JOINT VENTURE PARTNERS

HyperCube will share CPNI with a partner, vendor contractor or third party agent only after that person or entity has entered into a confidentiality agreement with the Company. The confidentiality agreement must include the following:

HYPERCUBE TELECOM, LLC
CUSTOMER PROPRIETARY NETWORK INFORMATION ("CPNI")
PROTECTION POLICY

- require that the partner, contractor or agent use the CPNI only for the purpose of marketing or providing the Communications-Related Services for which it was provided;
- disallow the partner, contractor or agent from using, allowing access to or disclosing the CPNI to any other party, unless required to make such disclosure under force of law;
- require that the partner, contractor or agent have appropriate protections in place to ensure the ongoing confidentiality of the customer's CPNI; and
- require that the partner, contractor or agent notify HyperCube in the event that there is a breach involving a HyperCube customer's CPNI.
- **All such agreements must be approved** by HyperCube's CPNI Policy Administrator as identified in the box on Page 3.
- All third parties, including partners, vendor contractors or third party sales and marketing agents are prohibited from using CPNI for marketing purposes.

VII. RETENTION AND WIN-BACK

A. Restrictions on use of Carrier Proprietary Information to retain customers.

- If the Company learns by receipt of another carrier's order to switch the customer, or another carrier's change request, that a customer plans to switch from HyperCube to another carrier, HyperCube prohibits its employees, Company/legal agents, or affiliates from using that information to attempt to dissuade the subscriber from leaving.
- All HyperCube employees, legal/Company agents, or affiliates are prohibited from accessing a customers' call records for the purpose of identifying customers who may have called or been called by any of HyperCube's competitors.
- Subject to this policy statement on the use of CPNI, if the Company learns that a customer is switching to another carrier through an independent source (e.g., from a communication received directly from the customer or another independent source), CPNI may be used to persuade the customer to stay with HyperCube.

B. Win-back

- Subject to this policy on the use of CPNI, and as permitted by applicable Federal and state laws, HyperCube permits marketing campaigns to win back former customers that have switched to other carriers. If CPNI is used as part of a "win-back" campaign, it continues to be governed by this policy statement.

HYPERCUBE TELECOM, LLC
CUSTOMER PROPRIETARY NETWORK INFORMATION ("CPNI")
PROTECTION POLICY

- If a HyperCube employee, legal/Company agent or affiliate has any questions concerning whether it is appropriate to use CPNI or Carrier Proprietary Information (CPI) to market, retain or win-back a customer, please contact HyperCube's CPNI Policy Administrator as identified in the box on Page 3.

VIII. TRAINING AND REPORTING

A. Training Requirements

- HyperCube will provide a means for all its employees, legal/Company agents and affiliates to receive training in the proper uses of CPNI, including a familiarity with this policy statement. ***Please note that training and understanding with respect to proper use and protection of CPNI is critical, as failures to comply with any part of this policy may result in disciplinary action.*** Anyone who has not received the required training should contact HyperCube's CPNI Contacts identified in the box on Page 3.

B. Reporting Requirements

- HyperCube's CPNI Policy Administrator as identified in the box on Page 3 is responsible for all government reporting requirements in connection with CPNI.
- In the event that HyperCube ever offers an opt-out notice to its customers, it will provide a written report to the FCC of any instance in which the opt out method has failed to work properly, to such a degree that consumers' inability to opt out is more than an anomaly. The Company's report will be filed with the FCC within five business days after learning of such failure. Any employee who becomes aware of any malfunction in the opt-out system should immediately report it to HyperCube's CPNI Policy Administrator as identified in the box on Page 3.
- HyperCube is subject to strict reporting obligations to certain Federal authorities as soon as practicable in connection with maintenance, use, disclosure, breach or misuse of CPNI. *If you become aware of any unauthorized disclosure of CPNI or breach of any database containing any CPNI, you must immediately report such information to HyperCube's CPNI Policy Administrator as identified in the box on Page 3. You must also promptly confirm receipt of the email notification by the legal department.*

C. Notification of Account Changes

- The Company must notify a customer immediately whenever a password, customer response to a back-up means of authentication for lost or forgotten password, online account, or address of record is created or changed. Upon initial establishment of every Customer account, HyperCube requires its Customers to identify at least one primary contact with his or her email address. In the event that a Customer later reports to HyperCube a lost or forgotten password, HyperCube communicates with the Customer solely through that email address in order to perform a password reset, and HyperCube immediately

HYPERCUBE TELECOM, LLC
CUSTOMER PROPRIETARY NETWORK INFORMATION ("CPNI")
PROTECTION POLICY

forwards to that email address a confirmation that the password has been reset. Changes to the address of record will also be confirmed via the email of record.

IX. RECORD-KEEPING REQUIREMENTS

HyperCube will maintain records of all sales and marketing campaigns, if any, that involve the use, disclosure or giving of permission for access to customers' CPNI, including those of the Company's affiliates or third parties. All such records will include a description of the campaign, identification of the CPNI used, and a listing of the products and services being offered to customers. One-time uses of CPNI are not generally considered to be sales or marketing campaigns, and individualized records of such one-time uses are not required, except that every disclosure of CPNI to a person or entity outside of HyperCube must be documented and recorded with the same information that would be required in a sales or marketing campaign. The records required under this paragraph will be maintained for a minimum of one year. Records will be maintained and approved by HyperCube's CPNI Policy Administrator as identified in the box on Page 3. HyperCube must maintain a record for a minimum of one year of its supervisory review process associated with any outbound marketing campaigns that use its customers' CPNI.

X. Breach Notification

If any Company employee learns of the use of CPNI, such information must immediately be brought to the attention of supervisory personnel. The Company has a duty to notify law enforcement of breaches involving customer CPNI as soon as practicable, and in no event later than seven (7) business days, after reasonable determination of the breach. Notifications are submitted electronically to the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) via the following web portal: <http://www.fcc.gov/eb/cpni>.

After notifying law enforcement, no earlier than 7 full business days after such notification (and longer if law enforcement requests), the Company must notify affected customers of the breach. The Company, in rare circumstances, may notify a customer earlier if there is an urgent need to provide such information to the customer and law enforcement has been notified of such need.

The Company maintains a record of all breach notifications for at least two years. Such records include, where available, the following information: dates of breach discovery and notification; a detailed description of the CPNI that was the subject of the breach; and the circumstances of the breach.

XI. HOW MAY CPNI BE USED WITH THE CUSTOMER'S APPROVAL AND HOW THAT APPROVAL MUST BE OBTAINED

There are a number of circumstances under which it is permissible for HyperCube to use CPNI as long as the customer has approved such use. Where customer approval is required,

HYPERCUBE TELECOM, LLC
CUSTOMER PROPRIETARY NETWORK INFORMATION ("CPNI")
PROTECTION POLICY

HyperCube must use either opt-out and opt-in approval as described below. ***Currently, HyperCube is not using CPNI in any manner that requires approval from its customers. In the event that changes, the CPNI Compliance Officer, Ronald Beaumont, will ensure that applicable HyperCube employees are notified and that the below procedures in Sections XI, XII, XIII and XIV are implemented.***

A. Opt-Out Approval

- The "opt out" approval method requires that the customer receive an individual notice (by written or electronic means) that the Company intends to use the customer's CPNI. Such notices must be sent by the Company 30 days before the customer's approval to use CPNI is inferred (33 days for notices sent by mail). If the customer communicates to HyperCube that use of the CPNI is not approved, the Company will honor that customer's decision to "opt out." In limited cases, oral approvals may be allowed, as described below in the section entitled *Special Requirements Applicable to One-Time Oral Notices to Customers*.
- If the Company elects to send opt out notices by e-mail, the customer must previously have agreed to receive e-mails regarding their account. The subject line of the e-mail must clearly and accurately identify the subject (e.g. "Privacy of Your Phone Records"), and the customer must have the option of replying directly to the e-mail. If the e-mail is returned as undeliverable, HyperCube may not use the customer's CPNI until the required notice is given by another means. If the Company elects to send opt-out notices by e-mail, the customer must be able to opt out at no cost and be able to notify the Company of his or her decision on a 24-hour/7-day-per-week basis.
- Opt out approval must be refreshed every two years by sending a new notice, with a new 30 or 33 day waiting period for approval.
- If the customer has received notice and has given approval by the "opt out" procedure described above, CPNI may be used by HyperCube, its affiliates, subsidiaries and legal/Company agents, to market HyperCube's Communications-Related Services.

B. Opt-In Approval

- Opt-in Approval requires HyperCube to obtain from the customer an affirmative, express consent—in oral, electronic or written form—allowing the requested CPNI usage, disclosure or access, after receiving appropriate notification as described in Section XII below.
- Although customer approvals under the opt-in method may be obtained orally, HyperCube will allow oral approvals only with written authorization of the Company's management. If oral approval is received, the burden will lie on the Company to show that the customer received all of the information that would otherwise have been required in writing, and gave the necessary approval.

HYPERCUBE TELECOM, LLC
CUSTOMER PROPRIETARY NETWORK INFORMATION ("CPNI")
PROTECTION POLICY

- Opt-in consent must be obtained if HyperCube, its agents or affiliates or an unrelated third party uses a customer's CPNI to market a non-Communications-Related Service.
- Opt-in consent also must be obtained if a third party agent, vendor or contractor uses CPNI to market any service, including a Communications-Related Service, to a customer.

XII. NOTICE REQUIREMENTS APPLICABLE TO BOTH THE OPT-IN AND OPT-OUT METHODS OF APPROVAL

Opt-In and Opt-Out Notices to customers must be clearly written, legible, and provide sufficient information to enable the customer to make an informed decision to allow or deny use of CPNI. HyperCube must describe what CPNI is, how it is proposed to be used by the Company, and what specific entities may receive the CPNI if approval is granted. Although the notice may advise the customer that use or disclosure of CPNI will enhance HyperCube's ability to provide services to the customer, the notice must also state that the customer has the right, and HyperCube has the duty under Federal law, to protect the confidentiality of CPNI. The customer must be informed of his or her right to deny or later withdraw approval of HyperCube's proposed use of CPNI, and also be advised of the precise steps that must be taken in order to grant or deny approval of such use. Customers must be notified that denial of access to CPNI will not affect the provision of any services to which the customer subscribes.

XIII. SPECIAL REQUIREMENTS APPLICABLE TO ONE-TIME ORAL NOTICES TO CUSTOMERS

In general, one-time oral notices are appropriate when the Company has made a one-time inbound or outbound telephone contact with the customer and access to CPNI is useful to analyze the customer's existing service. In such cases, HyperCube may use oral notices to obtain limited, one-time use of CPNI *only for the duration of the call*, irrespective of whether the Company uses opt-out or opt-in approval with respect to that customer. When using the one-time oral notice method, the customer must be advised of the same information that would otherwise be provided in a written or electronic notice as provided above. However, certain information may be omitted from the oral notice, if it is clearly inapplicable, including: (a) notice that CPNI will be shared with affiliates or third parties; (b) the specific steps that are necessary to approve or restrict use of CPNI; and (c) notice that previous opt-out decisions require no further action to maintain the opt-out election. Notation should be made in the customer's record of any one-time oral notice to the customer and the customer's acceptance or rejection of one-time use of CPNI.

XIV. HOW TO VERIFY A CUSTOMER'S APPROVAL AND OBTAIN SUPERVISORY APPROVAL FOR PROPOSED OUTBOUND MARKETING EFFORTS

A. Customer Approval Database

HYPERCUBE TELECOM, LLC
CUSTOMER PROPRIETARY NETWORK INFORMATION ("CPNI")
PROTECTION POLICY

- If HyperCube changes its CPNI marketing practices such that customer approval is necessary, HyperCube will maintain a database that identifies whether or not a Customer has given approval for access to its CPNI. Employees, Company agents and affiliates are obligated to use that database before using, disclosing or permitting access to customers' CPNI and these persons may obtain the information in this database by contacting: HyperCube's CPNI Policy Administrator as identified in the box on Page 3. Company employees, agents and affiliates are prohibited from using, disclosing or permitting access to CPNI of any customer who is not listed in the database as having given approval. Moreover, any parties with access to CPNI have an obligation to protect CPNI from unauthorized access by other parties. Disciplinary action may result from violation of this prohibition.
- HyperCube will maintain records of such customer approval to use, access or disclose CPNI, whether oral, written or electronic, for a minimum of one year. A customer's approval or disapproval will remain in effect until the customer revokes or limits such approval or disapproval. These records will be generated by adding to a database each customer who does not approve the use of CPNI. This database will be maintained by HyperCube's CPNI Policy Administrator as identified in the box on Page 3. All customers who request that their accounts be CPNI restricted shall have a prominent indicator noted on all systems that permit account access.
- Please report any inaccuracies found in the customer approval database promptly to HyperCube's CPNI Policy Administrator as identified in the box on Page 3.

B. Supervisory Review Required Before Making a Request to a Customer

- Company employees, agents and affiliates must obtain supervisory review before making any request to a customer to use, disclose or permit access to CPNI. All requests for such review should be directed to HyperCube's CPNI Policy Administrator as identified in the box on Page 3. The review shall ensure that the requirements of this policy statement are followed.
- Notwithstanding the above, Customer Service Representatives (CSR) who receive in-bound calls from customers shall be allowed to access CPNI after receiving oral permission from the customer if the customer can provide specific detail about the reason for their call (e.g. when disputing a phone charge, if the customer provides date/time of the charge in question, the CSR may discuss that charge), and such permission shall be limited to the duration of the call. The CSR shall note on the account that the customer gave one-time oral permission to access CPNI, and that the permission ended when the call ended.

HYPERCUBE TELECOM, LLC
CUSTOMER PROPRIETARY NETWORK INFORMATION (“CPNI”)
PROTECTION POLICY

XV. GLOSSARY

Account information: Information that is specifically connected to a Customer’s service relationship with HyperCube. This information includes, among other things, account number, telephone number, and bill amount. Account information shall be treated as Customer Proprietary Network Information.

Address of Record: An “address of record,” whether postal or electronic, is an address that the carrier has associated with the customer’s account for at least 30 days.

Affiliate: A person that (directly or indirectly) owns or controls, is owned or controlled by, or is under common ownership or control with, another person. The term “own” means an equity interest (or the equivalent thereof) of more than 10 percent.

Aggregate Customer Information: Collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed.

Breach: When a person without authorization, or exceeding authorization, intentionally gains access to, uses, or discloses CPNI.

Call Detail Information: Any information that pertains to the transmission of specific telephone calls including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call.

Carrier Proprietary Information (CPI): A request from one carrier to another to *switch* a customer.

Communications-Related Services: Telecommunications services, information services typically provided by telecommunications carriers, and services related to the provision and maintenance of customer premises equipment. Information services that are typically provided by telecommunications carriers include Internet access and voice mail services. Retail consumer services provided by use of Internet websites (such as travel reservation services or mortgage lending services), are not typically provided by telecommunications carriers and are not considered Communications-Related Services, whether or not such services may otherwise be considered to be information services.

Customer: For purposes of this manual, a customer is a person or entity receiving telecommunications service from HyperCube.

HYPERCUBE TELECOM, LLC
CUSTOMER PROPRIETARY NETWORK INFORMATION ("CPNI")
PROTECTION POLICY

Customer Proprietary Network Information (CPNI): Information (a) that relates to the quantity, technical configuration, type, destination, location and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; or (b) that is contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; except that such term does not include subscriber list information.

Opt-in approval: A method for obtaining customer consent to use, disclose, or permit access to the customer's CPNI. This approval method requires that the carrier obtain from the customer affirmative, express consent allowing the requested CPNI usage, disclosure, or access after the customer is provided appropriate notification of the carrier's request consistent with the requirements set forth in this subpart.

Opt-out approval: A method for obtaining customer consent to use, disclose, or permit access to the customer's CPNI. Under this approval method, a customer is deemed to have consented to the use, disclosure, or access to the customer's CPNI if the customer has failed to object thereto within a certain waiting period.

Subscriber List Information (SLI): Any information of a HyperCube subscriber (such as name, address, telephone number or classification) that the Company or an affiliate has published, caused to be published, or accepted for publication in a directory.

Telecommunications Carrier or Carrier: As set forth in Section 3(44) of the Communications Act of 1934, as amended. Generally, a telecommunications carrier is a provider of transmission services directly to the public for a fee, between or among points specified by the user, without change in the form or content of the information as sent and received. HyperCube is a telecommunications carrier.